UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P O Box 1450
Alexandria, Virginia 22313-1450
www uspto gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/510,606	05/19/2005	Eric Diehl	PF020035	3927

24498 7590 02/02/2009

Robert D. Shedd
Thomson Licensing LLC
PO Box 5312
PRINCETON, NJ 08543-5312

EXAMINER	
SHIFERAW, ELENI A	

ART UNIT	PAPER NUMBER
2436	

MAIL DATE	DELIVERY MODE
02/02/2009	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	**Application No.** 10/510,606	**Applicant(s)** DIEHL ET AL.	
	Examiner ELENI A. SHIFERAW	**Art Unit** 2436	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *12 November 2008*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-2 and 4-13* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1,2 and 4-13* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☐ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____.

4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) ☐ Notice of Informal Patent Application

6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-2 and 4-13 are pending.

2. Applicant cancels claim 3.

3. Claims 1, 5-6, 9, and 11 are amended.

Information Disclosure Statement

4. The information disclosure statement (IDS) submitted on 10/08/2004 has been considered. The submission is in compliance with the provisions of 37 CFR 1.97. Form PTO-1449 is signed and attached hereto.

Priority

5. Acknowledgment is made of applicant's claim for foreign priority under 35 U.S.C. 119(a)-(d). The certified copy has been filed in parent Application No. 10510606, filed on 10/08/2004.

Oath/Declaration

6. The oath filed on 05/19/2005 complies with all the requirements set forth in MPEP 602 and therefore is accepted.

Drawings

7. The drawings filed on 10/08/2004 are accepted.

Response to Amendment

8. The amendment to the abstract is accepted and objection is herein withdrawn.

9. The amendment to the specification is accepted and objection is herein withdrawn.

10. The amendment to the claims (claims 1 and 5) is accepted and objection is herein withdrawn.

Response to Arguments

11. Applicant's arguments filed 11/12/2008 have been fully considered but they are not persuasive.

Regarding argument the references failure to teach "to send an identifier from the receiver to the transmitter" as recited in claim 1, remark page 8 last par., argument is not persuasive because Menezes discloses a method of data integrity or authentication on the messages transmitted between transmitter/sender/claimant (A) and receiver (B) see section 10.16-10.17. **Menezes further discloses generating random numbers rA and rB that is based on A's identifier and B's identifier, respectively and that is random numbers and identifiers of A and B are exchanged**

(see section 10.16-10.17 wherein … rA and tA respectively denote a random number and a timestamp generated by A… Ek denotes a symmetric encryption algorithm … **It is assumed both parties are aware of the claimed identity of the other, either by context or by additional (unsecured) clear text data fields.** Optional message fields are denoted by an asterisk (*), ...

1. unilateral authentication, timestamp-based:

   A→B : Ek(tA,B*)

   Upon reception and decryption, B verifies that the timestamp is acceptable and optionally ***verifies the received identifier*** as its own. **The identifier B** here prevents …..

2. unilateral authentication, using ransom numbers:

   To avoid reliance on timestamp…..

   A← B : rB
   A→B : Ek(rB, B*)

   B decrypts the received message and checks that the random number matches that is sent. Optionally, ***B checks that the identifier (received) is its own***….

3. mutual authentication using ransom numbers:

   A ← B : rB

   A → B : Ek(rA, rB, B*)

A ← B : Ek(rB,rA) ...

10.17 Remark (doubling unilateral authentication) ......

(ii) Challenge-response based on (keyed) one-way functions

....

3. to enable independent MAC computation by the recipient, the additioanl cleartext field tA must be sent in message of the one-pass mechanism.

The revised three-pass challenge-response mechanism based on a MAC hk, with actions as noted above provide mutual identification. ...

A ← B : rB
A → B : rA; hk(rA,rB,B)
A ← B : hk(rB,rA,A) ...)

Regarding argument Menezes failure to disclose "receiving from the transmitter a response computed by applying a first function to said random number and to said identifier;" argument page 9 par. 1, argument is not persuasive because Menezes on page 401-402 sec. 10.16 line 25 discloses B receiving Ek(rB,B*) wherein rB is random number and identifier.

Regarding argument Menezes failure to teach "verifying the received response by applying a second function to the received response, to said random number and to said identifier" remark page 9 par. 2, argument is not persuasive because see section 10.16-10.17 of Menezes wherein disclosed B decrypting the received message using a decryption function, and checking/verifying that the random number matches that sent and checking that the identifier is its own and further confirm the integrity of the message.

Therefore Menezes discloses every single limitation of b, c, and d.

Regarding argument Haumont and Teper failure to teach steps b, c, and d wherein "broadcasting from a receiver of data, a random number and an identifier over a network, receiving from the transmitter a response computed by applying a first function to the random number and to the identifier, and verifying the received response by applying a second function to the received response, to the random number and to the identifier" remark page 10 par. 2 and page 11 last par., argument is not persuasive because one cannot show nonobviousness by attacking references individually where the rejections are based on combinations of references. See *In re Keller*, 642 F.2d 413, 208 USPQ 871 (CCPA 1981); *In re Merck & Co.,* 800 F.2d 1091, 231 USPQ 375 (Fed. Cir. 1986).

Claim Rejections - 35 USC § 103

12. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

13. Claims 1-2, 5, 7-8, 10, and 12-13 are rejected under 35 U.S.C. 103(a) as being unpatentable over Menezes "Handbook of applied cryptography" in view of Haumont USPN 6763112 B1.

Regarding claim 1, Menezes discloses a method for verifying that data received by a receiver (pp 401 sec. 10.16; *data integrity/authentication ... and receiver (B)*) have been sent by a transmitter (*sender/claimant (A))* authorized by a trusted third party (pp 400 sec. 10.3.2 lines 1-7; *trusted on-line server*), the transmitter and the receiver being connected to a digital network (pp 400 sec. 10.3.2 lines 1-7 and pp 401 sec. 10.16 lines 1-27), wherein an identifier is associated with the data sent by the transmitter (pp 401 sec. 10.16 lines 7-page 402 lines 8; *B checking the identifier in equation (2) is its own... random number rB is based on B's identity... same for A i.e. rA is based on A's identity*) the method, for the receiver comprising:

(a) generating a random number (pp 401 sec. 10.16 lines 7-24; *random number is generated...rA, rB)*;

(b) broadcasting said random number and said identifier over the network (pp 401 sec. 10.16 line 24; *equation (1) and/or rB is transmitted to A .... rB is based on B's identifier ...* pp 401 sec. 10.16 lines 11-pp 402 sec. 10.17 (ii); *rA and rB are exchanged between A and B*);

(c) receiving from the transmitter a response computed by applying a first function to said random number and to said identifier (pp 401 sec. 10.16 line 25; *equation (2) and/or Ek(rB,B*)*); and

(d) verifying the received response by applying a second function to the received response, to said random number and to said identifier (pp 401 sec. 10.16 lines 9-31; *B decrypts Ek(rB,B*) using decryption algorithm Ek and checks/verifies the integrity and identity using random number sent*).

Menezes discloses the trusted on-line server providing common session key (see pp 400 sec. 10.3.2 lines 3-7 to A and B) and algorithm Ek that denotes symmetric encryption algorithm with a key K is shared by A and B see pp 401 sec. 10.16 lines 9-11, and the algorithm Ek is used in A and B for security and/or verification (see pp 401 sec. 1016 lines 1-27).

However Menezes fails to explicitly disclose the Ek being transmitted to A and B from the trusted on-line server.

Haumont discloses a method of trusted third party (CN) transmitting UMTS Integrity Algorithm (UIA) and UMTS Encryption Algorithm (UEA) to mobile station (MS) or radio network controller (RNC) (col. 5 lines 65-col. 6 lines 2), via distributed network (see fig. 1 and col. 4 lines 46-65), for proper challenge response authentication integrity result (see col. 5 lines

4-32 and fig. 2) and integrity is verified by transmitting challenge/random from CN to MS, in response to the received challenge the MS applying algorithm to produce a result, transmitting the generated result to CN and acknowledging the RNC (see col. 6 lines 3-24 and fig. 4 and fig. 2).

Therefore it would have been obvious to one having ordinary skill in the art at the time of the invention was made to modify the teachings of Haumont within the system of Menezes because they are analogous in challenge response integrity authentication. One would have been motivated to incorporate the teachings to properly perform integrity authentication using the trusted algorithm.

Regarding claim 5, Menezes discloses a method for proving that data sent to a receiver (pp 401 sec. 10.16; *data integrity/authentication ... and receiver (B)*) have been transmitted by a transmitter (*sender/claimant (A))* authorized by a trusted third party (pp 400 sec. 10.3.2 lines 1-7; *trusted on-line server*), the transmitter and the receiver being connected to a digital network (pp 400 sec. 10.3.2 lines 1-7 and pp 401 sec. 10.16 lines 1-27), characterized in that wherein an identifier is associated with the data sent by the transmitter (pp 401 sec. 10.16 lines 7-page 402 lines 8; *B checking the identifier in equation (2) is its own... random number rB is based on B's identity... same for A i.e. rA is based on A's identity*) the method, for the transmitter comprising:

(a) receiving a random number from the receiver (pp 401 sec. 10.16 line 24; *equation (1) and/or rB is received at A*);

(b) computing a response by applying a first function to said random number and to said identifier (pp 401 sec. 10.16 lines 9-31; *equation (2) and/or Ek(rB,B*) wherein Ek is the encryption algorithm and rB is based on B's identity*); and

(c) sending said response to the receiver (pp 401 sec. 10.16 line 25; *equation (2))*;

said response being verified by the receiver by applying a second function to the received response, to said random number and to said identifier (pp 401 sec. 10.16 lines 9-31; *B decrypts Ek(rB,B*) using decryption algorithm Ek and checks/verifies the integrity and identity using random number rB sent that is based on B's identity*).

Menezes discloses the trusted on-line server providing common session key (see pp 400 sec. 10.3.2 lines 3-7 to A and B) and algorithm Ek that denotes symmetric encryption algorithm with a key K is shared by A and B see pp 401 sec. 10.16 lines 9-11, and the algorithm Ek is used in A and B for verification (see pp 401 sec. 1016 lines 1-27).

However Menezes fails to explicitly disclose the Ek being transmitted to A and B from the trusted on-line server.

Haumont discloses a method of trusted third party (CN) transmitting UMTS Integrity Algorithm (UIA) and UMTS Encryption Algorithm (UEA) to mobile station (MS) or radio network controller (RNC) (col. 5 lines 65-col. 6 lines 2), via distributed network (see fig. 1 and col. 4 lines 46-65), for proper challenge response authentication integrity result (see col. 5 lines 4-32 and fig. 2) and integrity is verified by transmitting challenge/random from CN to MS, in response to the received challenge the MS applying algorithm to produce a result, transmitting the generated result to CN and acknowledging the RNC (see col. 6 lines 3-24 and fig. 4 and fig. 2).

Therefore it would have been obvious to one having ordinary skill in the art at the time of the invention was made to modify the teachings of Haumont within the system of Menezes because they are analogous in challenge response integrity authentication. One would have been motivated to incorporate the teachings to properly perform integrity authentication using the trusted algorithm.

Regarding claim 2, Menezes discloses the method in which the step (b) is replaced by a step consisting in sending said random number to the transmitter (pp 401 sec. 10.16 line 24-pp 402 line 8; *rB*).

Regarding claim 7, Menezes discloses the method wherein the identifier associated with the data sent by the transmitter is a random number generated by the initial transmitter of the data in the network and attached to said data by the initial transmitter (pp 401 sec. 10.16 lines 7-page 402 lines 8; *B checking the identifier in equation (2) is its own using random number rB… random number rB is based on B's identity… same for A i.e. rA is based on A's identity*).

Regarding claim 8, Menezes discloses the method wherein the first function is a public function using a secret key (pp 402 sec. 10.17 lines 9-34; *hk is a one-way hash function that is known to both the sender and receiver and uses a shared key/secret key*).

Regarding claim 10, Menezes discloses the method wherein the first function is a secret function (pp 402 lines 1-8; *algorithm Ek is used that prevents chosen-text attacks*).

Regarding claim 12, Menezes discloses the method wherein the first function is a public function for signature generation with the aid of a private key (pp 404 sec. (ii) lines 11; *SA*).

Regarding claim 13, Menezes discloses the method wherein the second function is a public function for signature verification with the aid of a public key corresponding to the private key used by the first function (pp 404 sec. (ii)-pp 405 lines 18; *SA is signature algorithm for verification with the aid of public key-private key*).

14. Claims 4, 6, 9 and 11 are rejected under 35 U.S.C. 103(a) as being unpatentable over Menezes "Handbook of applied cryptography" in view of Haumont USPN 6763112 B1. and further in view of Teper et al. USPN 5815665.

Regarding claim 4, the combination of Menezes and Haumont discloses all the subject matter as discloses above. The combination is silent in details of inhibiting access to said data if the response received in the step (c) is not correct or if no response is received after the expiry of a predetermined time starting from the transmission of the random number.

However Teper et al. teaches a method for a user to connect to a service provider (SP) site and attempt to access an online service and the SP initiating a challenge-response authentication that allows an online brokering service to authenticate the user for the SP site, SP sending challenge message to the user's computer over the distributed network/Internet, user generating and returning response message that is based on the challenge message received and user's identifier/password and the response is authenticated for requested access and providing or denying access based on authentication result (see col. 9 lines 50-col. 10 lines 65 and col. 3 lines 5-44) that reads on a method wherein the receiver inhibits access to said data if the response received in the step (c) is not correct.

Therefore it would have been obvious to one having ordinary skill in the art at the time of the invention was made to combine the teachings of Teper et al. within the combination system because they are analogous in challenge response authentication. One would have been motivated to combine the teachings to securely provide access to authorized and authenticated user.

Regarding claim 6, the combination discloses the method in which the transmitter also receives in the step (a) said identifier associated with the data received by the receiver (see Menezes pp 401 sec. 10.16 lines 7-page 402 lines 8; *receiving rA and rB at B and A that are based on A's and B's identity*) and checking/authenticating A's and B's identifier in using challenge response message is also described see Menezes sec. 10.16 on page 401-402.

The combination is silent in wherein said in which the steps (b) and (c) are not carried out unless said identifier received in the step (a) corresponds to the identifier associated with the data that the transmitter has just sent.

However Teper et al. discloses a SP asking an online broker to authenticate a user by sending an encrypted pass-through message that includes user's response message, that is based on challenge response, and that includes the user's unique ID and the online broker looks up database for user's password based on the user's unique ID and determines whether the received response message corresponds to the user's password and the received challenge, generating correct response from the password and the received challenge message using same function used by the user computer and compare/authenticate the response message (see col. 10 lines 44-65 and col. 9 lines 50-67) that reads on in which the steps (b) and (c) are not carried out unless said identifier received in the step (a) corresponds to the identifier associated with the data that the transmitter has just sent.

Therefore it would have been obvious to one having ordinary skill in the art at the time of the invention was made to modify the teaching of Teper et al. within the combination system because they are analogous in challenge response authentication. One would have been motivated to do so to generate correct response and/or if the identifier does not match the receiver never generates same and authentic response as received response.

Regarding claim 9, the combination of Menezes and Haumont discloses authenticating and verifying data using challenge-response by applying to said random number and to said identifier the first function with the secret key (see Menezes pp 401 sec. 10.16). The combination is silent in giving details about the method wherein the second function is a boolean function and further comprising: computing an expected response and comparing the expected response with the response received in order to deliver: a "0" value if the expected and received responses are different and a "1" value if the expected and received responses are equal.

However Teper et al. discloses the method wherein the second function is a boolean function (see fig. 6 and col. 17 lines col. 18 lines 38)

computing an expected response (fig. 6 element 102) and comparing the expected response with the response received in order to deliver (fig. 6 element 104):

a "0" value if the expected and received responses are different (fig. 6 element 106; returning “No”) and

a "1" value if the expected and received responses are equal (fig. 6 elements 108-114; "yes").

Therefore it would have been obvious to one having ordinary skill in the art at the time of the invention was made to modify the teachings of Teper et al. within the combination system because they are analogous in generating a challenge response message and comparing the generated response with received for valid authentication. One would have been motivated to incorporate to grant/deny access based on the verification result.

Regarding claim 11, the combination discloses authenticating and verifying data using challenge-response by applying the first function to said random number and to said identifier (see Menezes pp 401 sec. 10.16). The combination is silent in giving details about the method wherein the second function is a boolean function and further comprising: computing an expected response and comparing the expected response with the response received in order to deliver: a "0" value if the expected and received responses are different and a "1" value if the expected and received responses are equal.

However Teper et al. discloses the method wherein the second function is a boolean function (see fig. 6 and col. 17 lines col. 18 lines 38)

computing an expected response (fig. 6 element 102) and comparing the expected response with the response received in order to deliver (fig. 6 element 104):

a "0" value if the expected and received responses are different (fig. 6 element 106; returning “No”) and

a "1" value if the expected and received responses are equal (fig. 6 elements 108-114; "yes").

Therefore it would have been obvious to one having ordinary skill in the art at the time of the invention was made to modify the teachings of Teper et al. within the combination system because they are analogous in generating a response message and comparing the generated response with received for valid authentication. One would have been motivated to incorporate to grant/deny access based on the verification result.

Conclusion

15. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

16. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. See PTO Form 892.

17. Any inquiry concerning this communication or earlier communications from the examiner should be directed to ELENI A. SHIFERAW whose telephone number is (571)272-3867. The examiner can normally be reached on Mon-Fri 8:00am-5:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nasser R. Moazzami can be reached on (571) 272-4195. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Eleni A Shiferaw/
Examiner, Art Unit 2436

/Nasser G Moazzami/
Supervisory Patent Examiner, Art Unit 2436